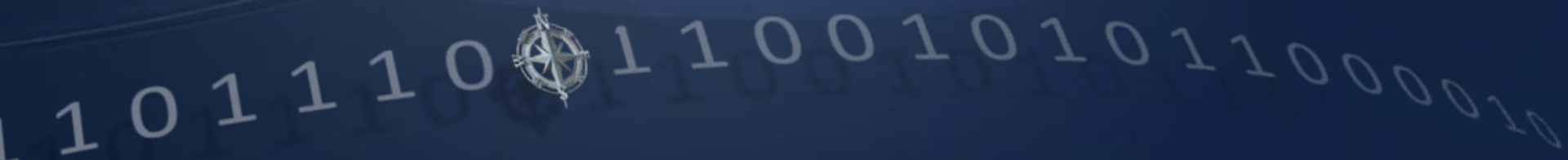




Consolidated Audit Program

PCI, HIPAA and SAS 70 for Service Providers

May 5th , 2010





- Kennet Westby, Chief Operating Officer
- Partner at Coalfire; Leads Auditing Service and serves as Senior Security Strategist
- 15 years of IT security and controls design and implementation experience
- Kennet has managed hundreds of risk-based compliance programs and IT audit engagements across multiple industries
- Maintains the following industry certifications: QSA, PA-QSA, CISA, CISSP and CISM

Agenda

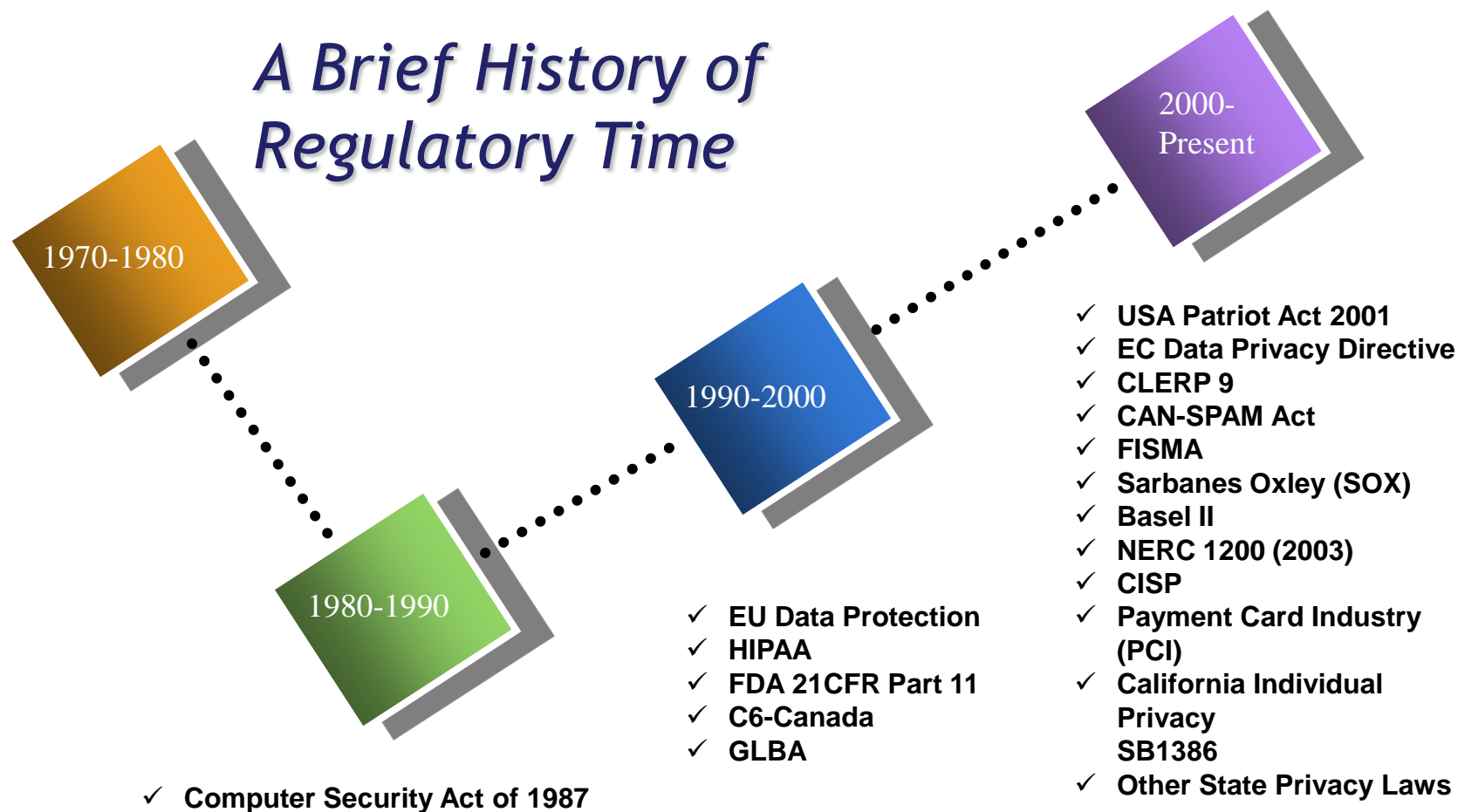
- Overview
- Challenges and Opportunities
 - Pressure on Service Providers
 - Problems with multiple compliance programs
 - Advantages of consolidated audit and compliance
- How to build a CAP program
 - Its all about the Information
 - Risk Assessment
 - Assemble the team
 - Establish the common controls
- Pre-audit readiness
- Audit and reporting
- Program maintenance
- Questions

Challenges for Service Providers

- Expanded Range of Service Providers needing compliance programs
 - SaaS offerings to retail, healthcare, life sciences and government are requiring compliance validation
 - Transactional processing, messaging, CRM, billing, ERP, data management are services bringing compliance in scope
 - Managed services and hosting providers must now demonstrate compliance and control validation
- Contracting is often driven by compliance validation and liability
 - Customers are demanding agreements include schedules of control responsibility and validation terms
 - Reporting of compliance and support of customer audit inquiry is taking significant resources
- Cost and Overhead
 - Service Providers are dedicating significant resources to manage multiple control and compliance validation programs

Increasing Regulation

A Brief History of Regulatory Time



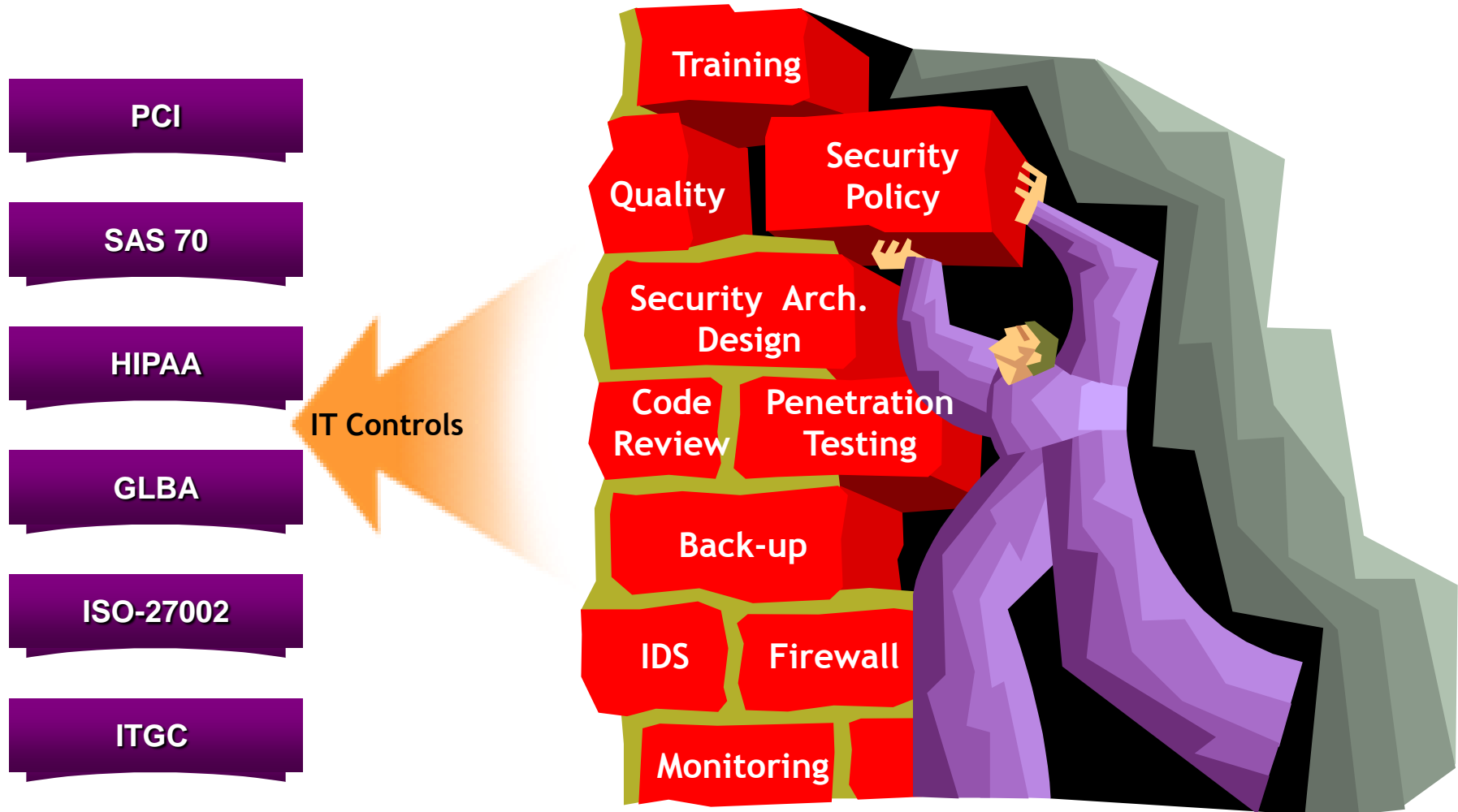
Maturing Expectations

- HITECH Changes
 - Service Providers are now responsible for HIPAA Security Rule compliance as a “Business Associate”
 - Civil and criminal HIPAA liability now apply to Service Providers
 - Customers are now demanding independent validation of HIPAA compliance within “Business Associate” agreements
- PCI ROC is Mandatory
 - Merchants and Bank Networks are demanding Level 1 ROC for any service provider supporting payment card processes
- SAS 70 Scope is Critical
 - Customers and their auditors are actually reading audit reports
 - If scope of controls do not address customer CIA requirements, customers and their auditors will not accept

Opportunity

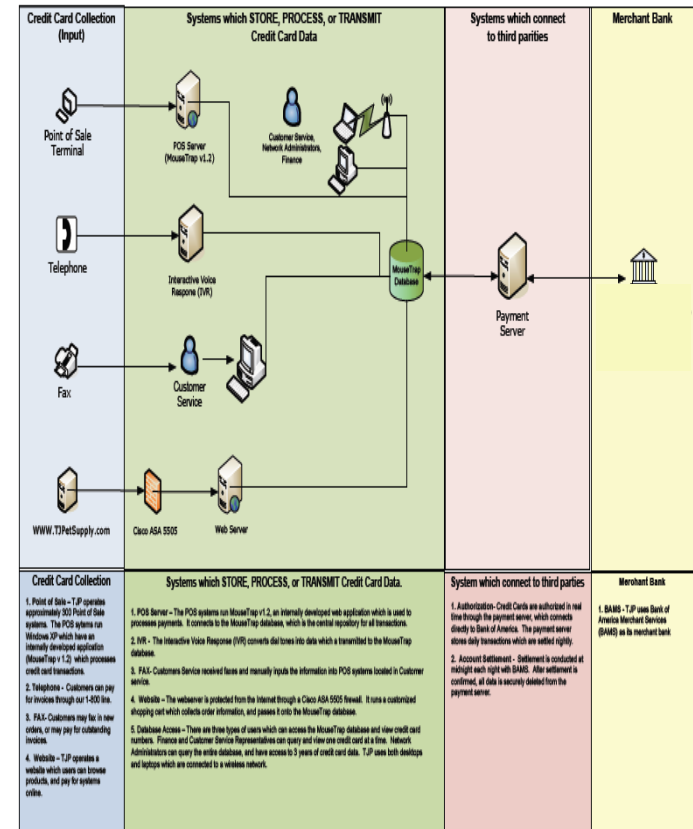
- Establish a single audit program
 - One yearly control audit can support all customer compliance reporting
 - Eliminate audit redundancy and inconsistency
- Establish a single control program
 - Addresses all risk and compliance objectives across confidentiality, integrity and availability
- Reduce control management and assessment costs
 - Maintain evidence consistently across cross to serve multiple audits or assessments
 - Shrink 3-6 months of separate audit programs into a single month of CAP
 - Free internal staff to focus on control management and improvement

Consolidation Challenge



All About The Data

- A Service Provider is governed by the data
 - Detailed data and process identification is critical
 - Information and supporting system assets define the scope of the control program
- Document process and information flow
 - All process scenarios are defined and documented
 - All networks, system assets, physical locations are documented with a clear understanding of data flow
 - All potential scenarios where PCI and PHI data could exist are documented



Risk Assessment

- Risk Assessment makes it all possible
 - A comprehensive and documented IT RA is the foundation for a successful CAP program
 - Rational for risk mitigation and risk acceptance is the glue that brings all individual programs and parties together
- Risk Management is what customers want demonstrated
 - PCI DSS is focused how control compliance has mitigated confidentiality risk to card data
 - HIPAA compliance must cover CIA risk to PHI
 - SAS 70 should focus on customer CIA risk across services
- Risk Assessment should establish highest common denominator
 - Risk management process will define the most stringent level of risk mitigation required to cover all risk instances
 - Compliance risk may not always be the highest bar

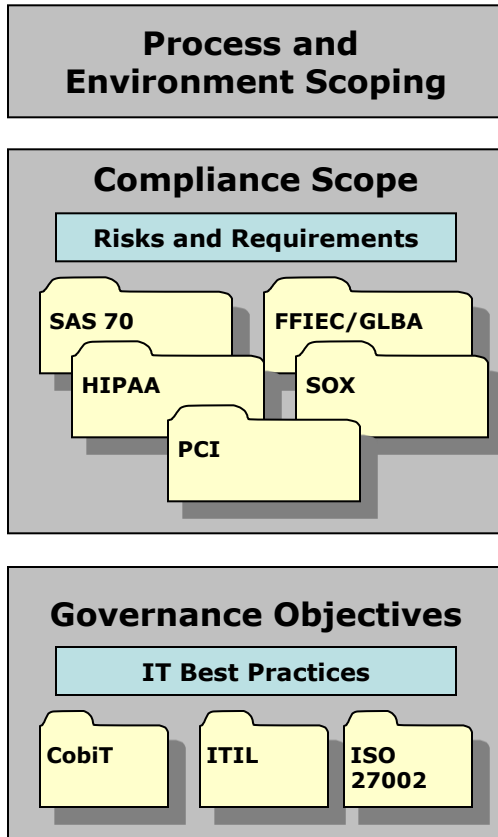
Assembling The Team

- Internal Team
 - Full management participation required
 - Cross-functional business and operational representation
 - Internal audit and risk management representatives
 - Legal and contracting are important
- External Team
 - PCI QSA auditors with service provider and HIPAA experience
 - AICPA auditor with PCI and HIPAA compliance experience
 - Cooperation and shared objectives from external auditors
- Resources and Tools
 - Control frameworks
 - Security testing services

Assembling The Program

CAP Project Management

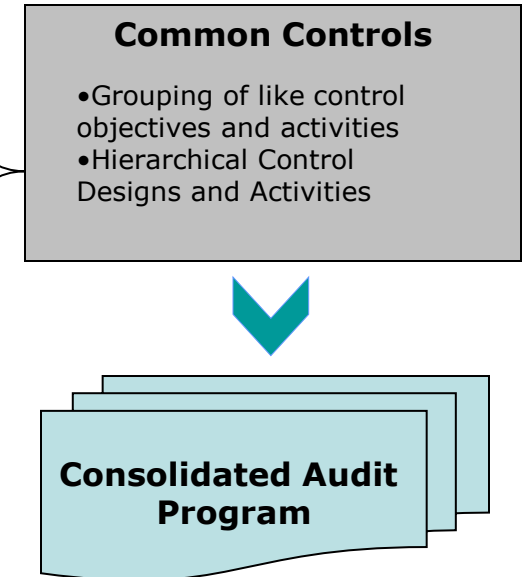
I. Extract Controls



II. Map Control Requirements

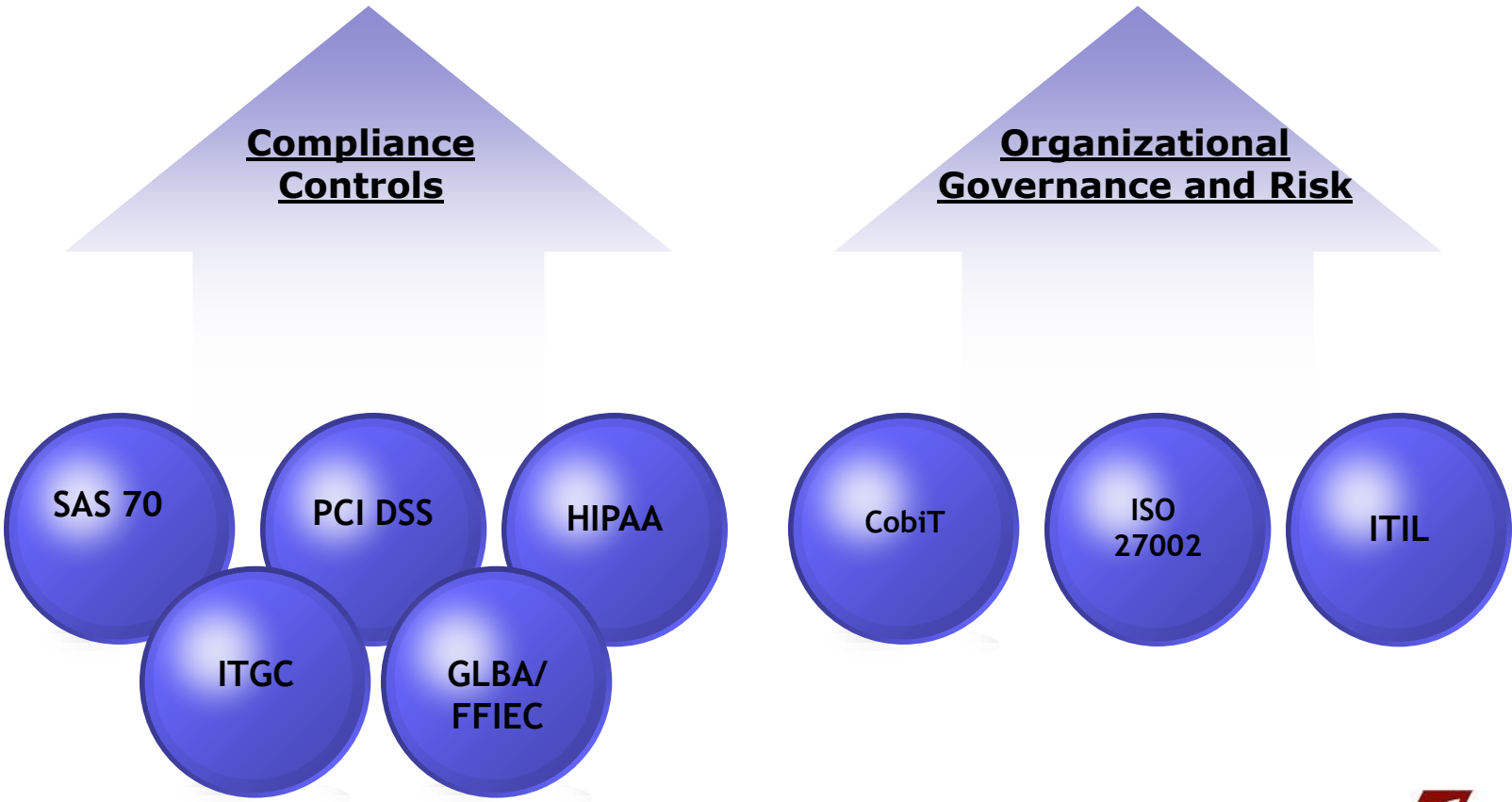


III. Assemble Framework



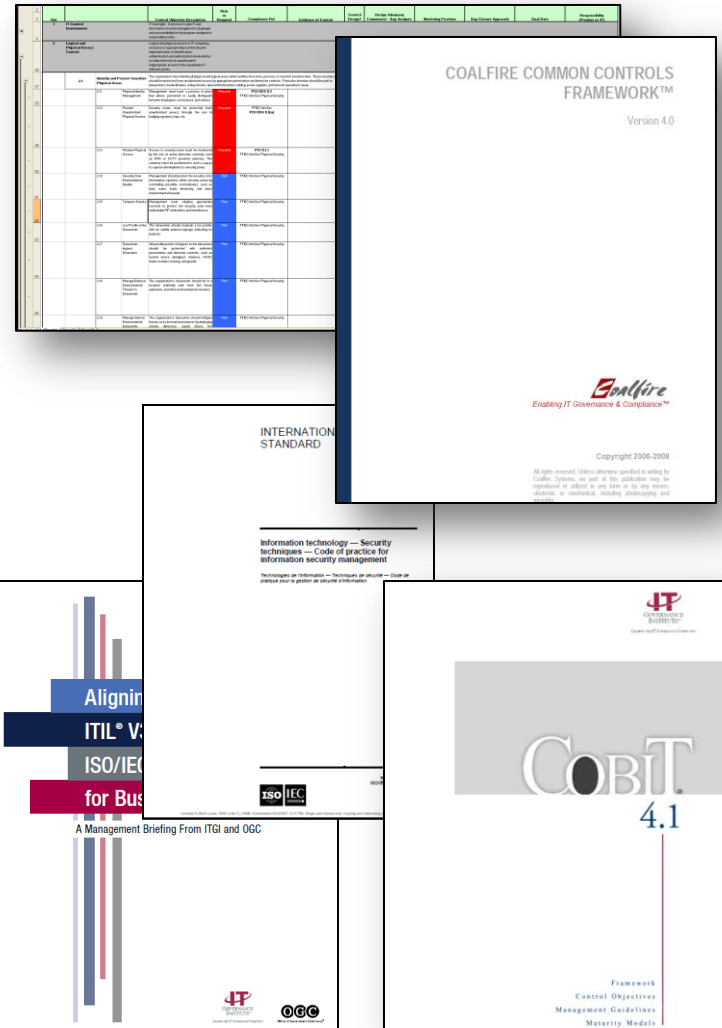
Common Controls Framework

Common Controls Framework



Tools and Resources

- Coalfire Common Controls
 - Framework that cross-walks all compliance and best practice control objectives
 - Provides audit guidance and IT asset mappings
 - 7 comprehensive control domains that cover governance, security, operations
- Cobit and Control Alignment
 - Control and Governance guidance
- Best Practice Frameworks
 - ISO 27002
 - ITIL
- GRC and Compliance Management Tools



Pre-Audit Readiness



- Validate process and data flow documentation
 - Information and IT asset identification and classification
 - Customer and third party interfaces
- Review risk assessment scope and risk management approach
 - Validate risk category definitions fulfill customer requirements
 - Corroborate any compliance scope reduction
- Establish consensus with all audit participants on control design, sampling, audit timeline and audit expectations
- Establish a single audit program for all control objectives with shared testing activities where required
- Coordinate audit plan and testing across audit team

Audit and Compliance Reporting

- Consolidated Audit Program should populate compliance and audit reporting for ROC, HIPAA Certification and SAS 70 Type 2 report output
- Audit reports are rendered by each qualified auditor/compliance assessment firm
- CAP maintains a reporting reference back to common audit program for all audit statements and findings
- Customers are provided a consolidated audit overview report that addresses all compliance requirements

Questions?

Kennet Westby
COO and Co-founder

Kennet.Westby@CoalfireSystems.com

877.224.8077 ext. 7502